10017328-1
Richard L. Schertz, et al.
System and Method of Graphically Displaying
Data for an Intrusion Protection System
4/4

REPLACEMENT
SHEET

FIG. 5

100

HP Netaction Attack Defender

File View Help

HP Attack Defender

122 — (Start) (Stop) (Reset)

| System |

(Back) **Detailed Results**
Ping of Death: 1 of 1 Prevented

| Intrusions |

Signature: (icmp) & (65535 < ((ip[2:2] - ((ip[0:1] 0x0f) * 4))
+ ((ip[6:2]_0x1fff) * 8)))) ← 102

| Attacks |

110

——————— ETHER Header ———————

| Recon |

ETHER: Destination: Accton-9A-0C-61 (00-00-E8-9A-0C-61)
ETHER: Source: 00-C0-4F-14-9D-81
ETHER: Protocol: IP ← 104

| SvcMgmt |

——————— IP Header ———————

| Policy |

IP: Version = 4
IP: Header length = 20
IP: Differentiated Services (DS) Field = 0x00   106
IP: 0000 00.. DS Codepoint = Default PHB (0)
IP: . . . . . .00 Unused

| Reports |

IP: Packet length = 1500 (1372 bytes missing) ~112
IP: Id = 10e1
IP: Fragmentation Info = 0x1FCC

| Log |

IP: .0.. .... Don't Fragment Bit = FALSE
IP: ..0. .... More Fragments Bit = FALSE
IP: ...1 1111 1100 1100 Fragment offset = 65120
IP: Time to live = 255

120

IP: Protocol = ICMP (1)
IP: Header checksum = 7066
IP: Source address = 10.1.1.2
IP: Destination address = 10.0.0.11
IP: Continuation of a missing packet   108

114

```
0000: 00 00 E8 9A 0C 61 00 C0 - 4F 14 9D 81 08 00 45 00    ....
0010: 05 DC 10 E1 1F CC FF 01 - 70 66 0A 01 01 02 0A 00    ....
0020: 00 0B 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00    ....
0030: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00    ....
0040: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00    ....
0050: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00    ....
0060: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00    ....
0070: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00    ....
0080: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00         ....
```